WARSS

Website **A**ttack **R**estoration **S**ecurity **S**olution

Защита веб-сайта в режиме реального времени

Содержание

umv

UMV Inc.

Основана в 2008 году

Сеул, Южная Корея

Веб-ориентированные решения

Безопасность веб-сервера в режиме реального времени

Предотвратить

Кража данных, прерывание работы веб-сервисов, порча веб-сайтов, постоянные атаки

Девиз

«Цепь безопасности сильна лишь настолько, насколько сильно ее самое слабое звено»

Почему WARSS?

https://www.youtube.com/watch?v=6gY1NWw9CJA&t=12s

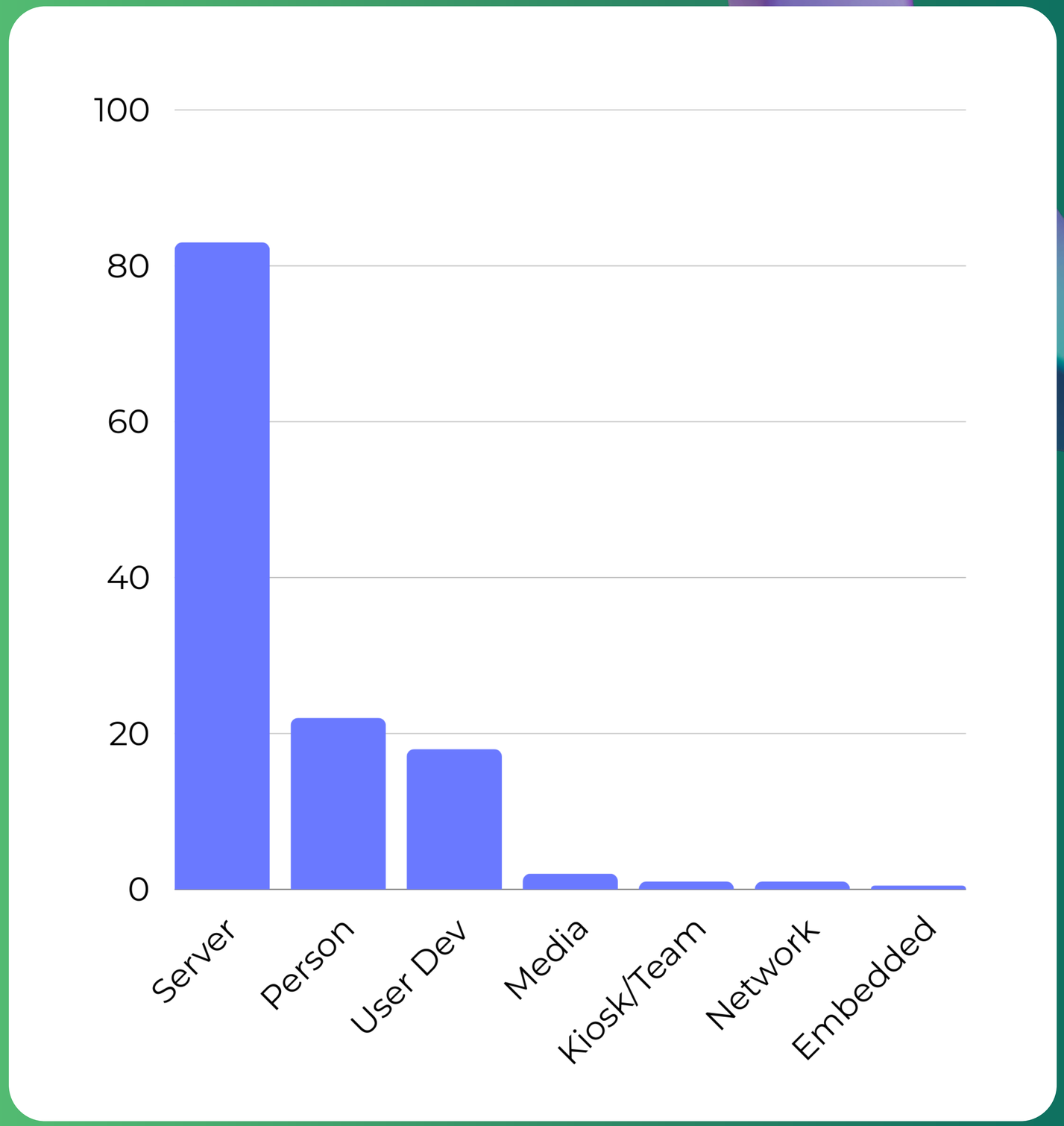
Веб-хакерство набирает обор

Verizon проанализировал рекордный **двухкратный** рост числа подтвержденных **нарушений безопасности** в период с 2022 по 2023 год.

Отчет о расследовании утечки данных Verizon за 2024 год

Активы, пострадавшие в результате нарушений

2023 Verizon DBIR



Взломаны украинские и российские сайты

Поддельные новости

Февраль 2024 г. — настоящее время:
Российско-украинская война сопровождается постоянными кибератаками друг на друга и союзников

Дезинформация и сбор данных

Целями являются предприятия малого и среднего бизнеса, средства массовой информации, государственные учреждения, ОТ и другие организации, обладающие личной/конфиденциальной информацией.

Недоверие: Ключ к кибервойнам

Публичность хакерских атак порождает страх, недоверие к властям и дезинформацию среди гражданского населения

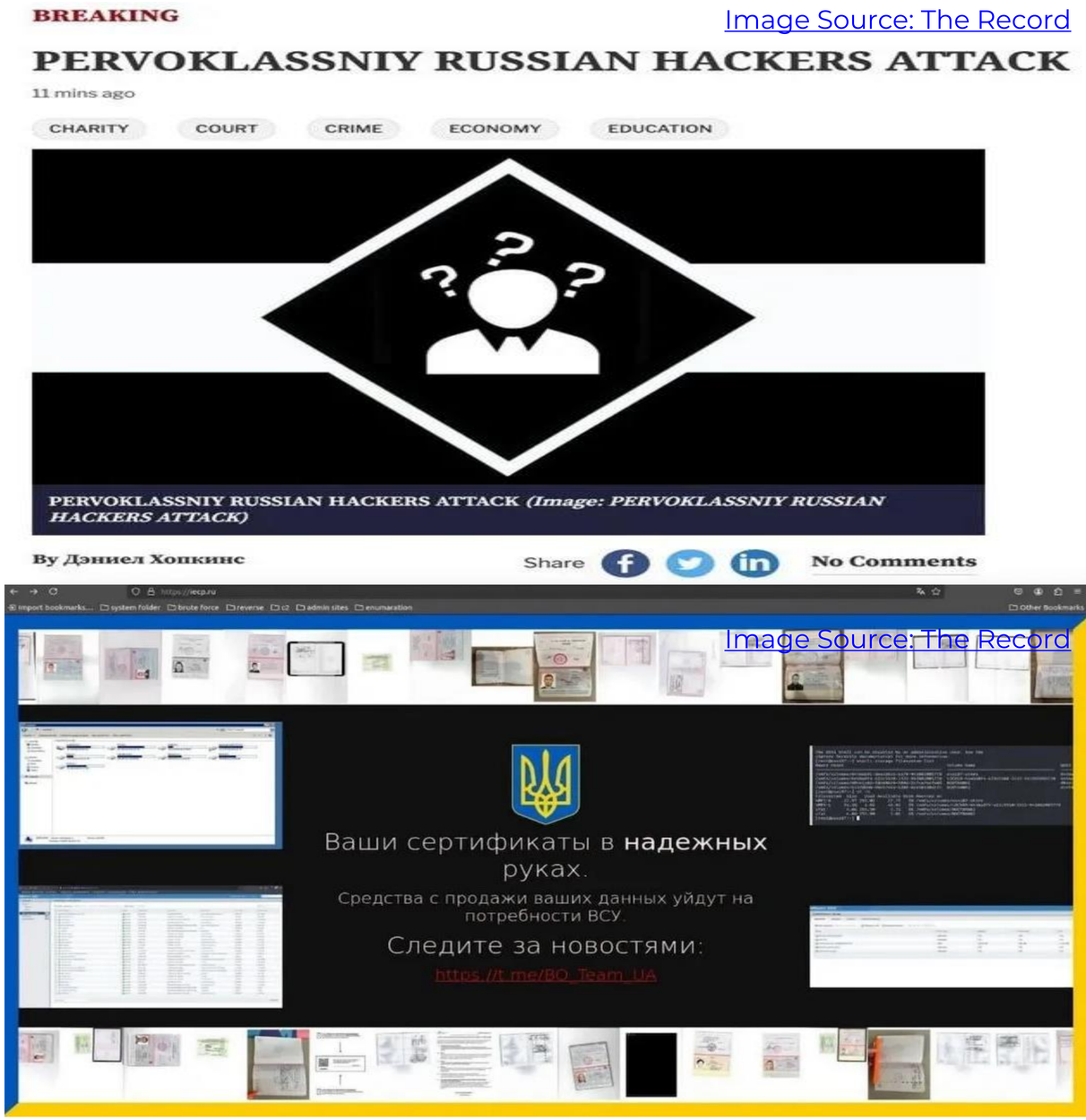


Image Source: The Record

Image Source: The Record

- https://therecord.media/ukrainian-news-outlets-attacked-by-russian-hackers
- https://therecord.media/russia-osnavanie-digital-signatures-cyberattack-ukraine

Атаки на Интернет-архив

Раунд 1: DDoS-атака, порча интерфейса, кража данных

9 октября 2024 года: DDoS-атака выводит сайт из строя; веб-сайт подвергся порче с использованием JavaScript-уведомления; имена пользователей, электронные адреса и другие данные 31 миллиона учетных записей утекли

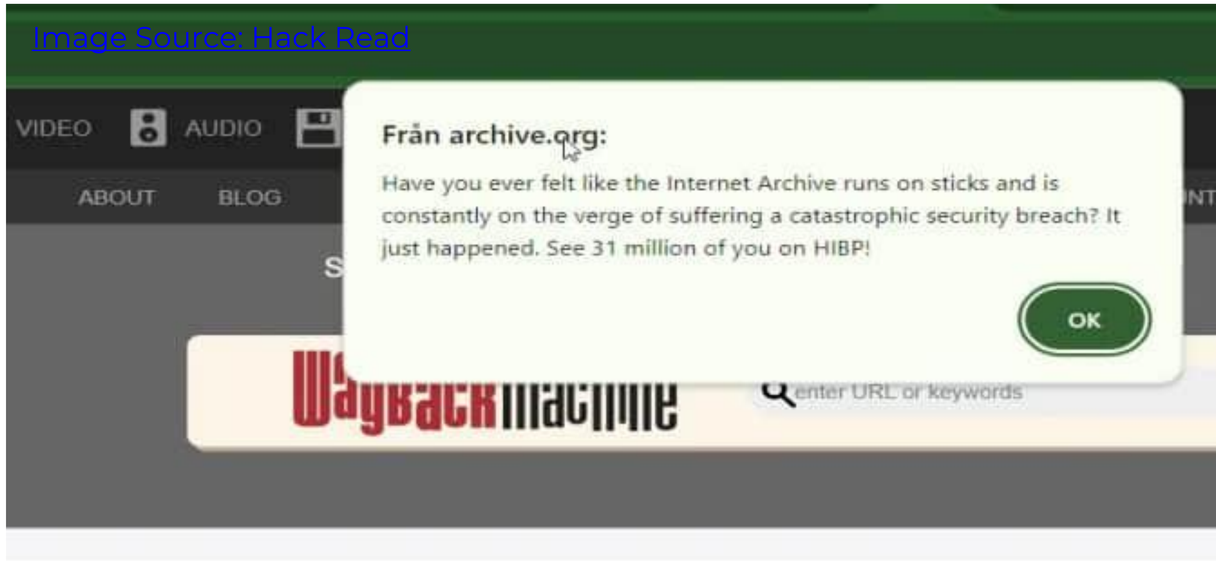
Обратно к первоначальному виду

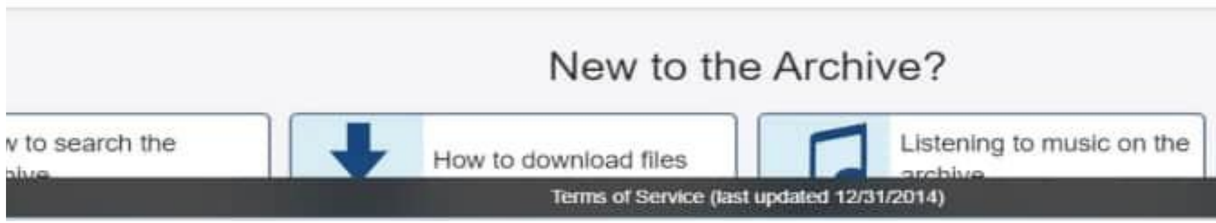
18 октября 2024 года: IA подтверждает, что данные в безопасности и услуги восстановлены

Раунд 2: Не защищенные цифровые ключи

20 октября 2024 года: Использование не обновленных токенов доступа для получения доступа к платформе поддержки Zendesk Интернет-архива; доступ к более чем 800 тыс. заявок в поддержку, начиная с **2018 года**

Image Source: Hack Read





- https://www.cbc.ca/radio/asithappens/internet-archive-hack-1.7359959
- https://therecord.media/internet-archive-data-breach-ddos-defacement
- https://hackread.com/internet-archive-archive-org-hacked-accounts-compromised/

Тренд: Хактивизм и кибертерроризм

- Взлом с целью продвижения политических или религиозных убеждений
- Увеличенная доступность платформ для зашифрованной связи (например, Telegram, Rocket Chat, Discord и т.д.) и **криптовалют**
    - **TRON** составил **около 90% средств,** связанных с **финансированием** терроризма с 2021 года (Форум новых технологий INTERPOL, октябрь 2023 года, Merkle Science)
- **Киберпреступность как услуга** (DDoS-атаки, программное обеспечение-вымогатели, учетные данные, данные и т.д.)

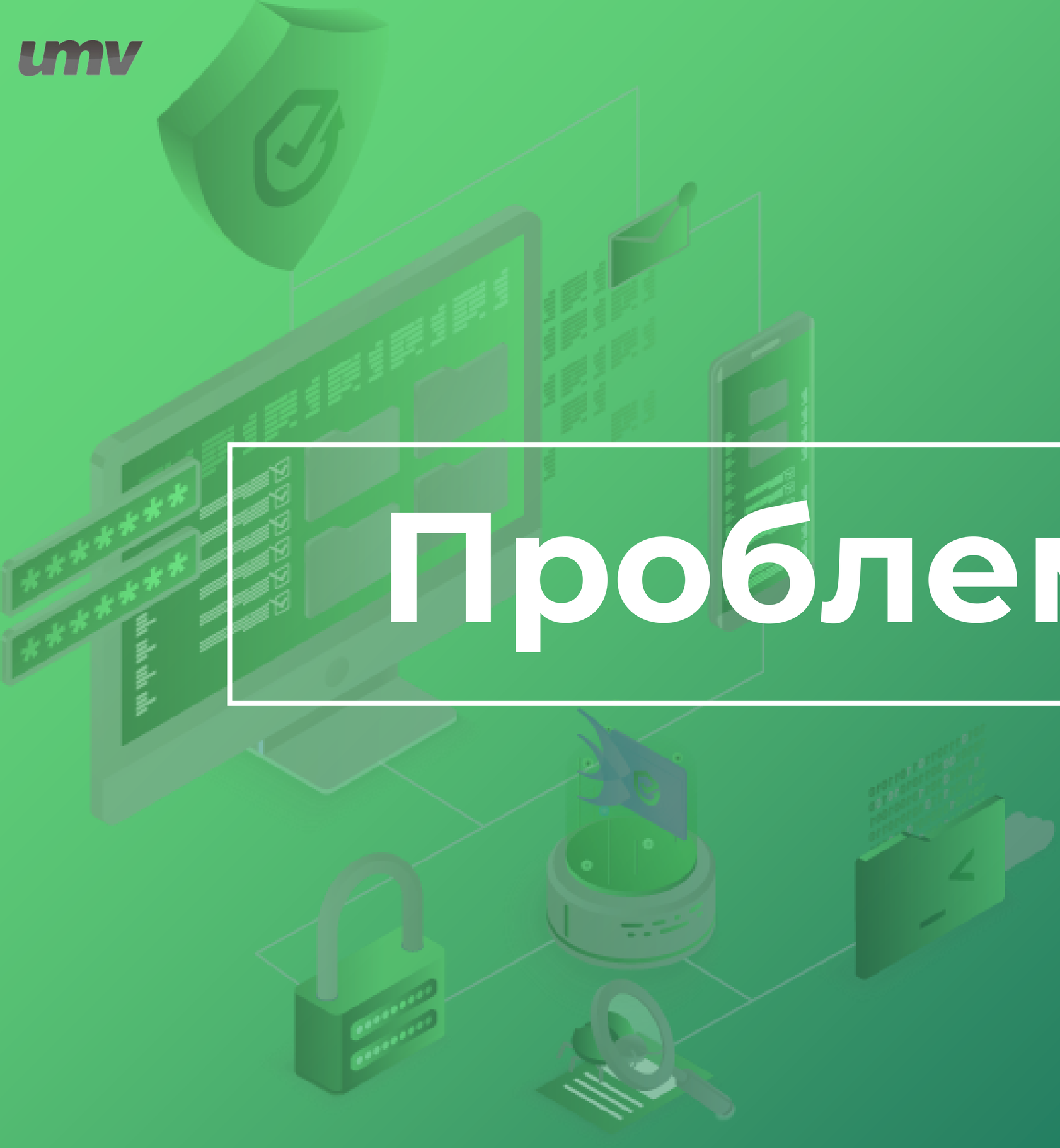
- *Отчет “the Surface Report”* (Июнь, 2024)
  UN Counter-Terrorism Centre (UNCCT)

Image Source: Malcontent News

Image Source: POLITICO

- https://unicri.it/sites/default/files/2024-06/DW.pdf

Проблема



Методы порчи веб-сайтов

1. Модификация исходного кода

Image Source: alphavilleherald.com

Image Source: boannews.com

Методы порчи веб-сайтов

2. Подделка контента/внедрение контента

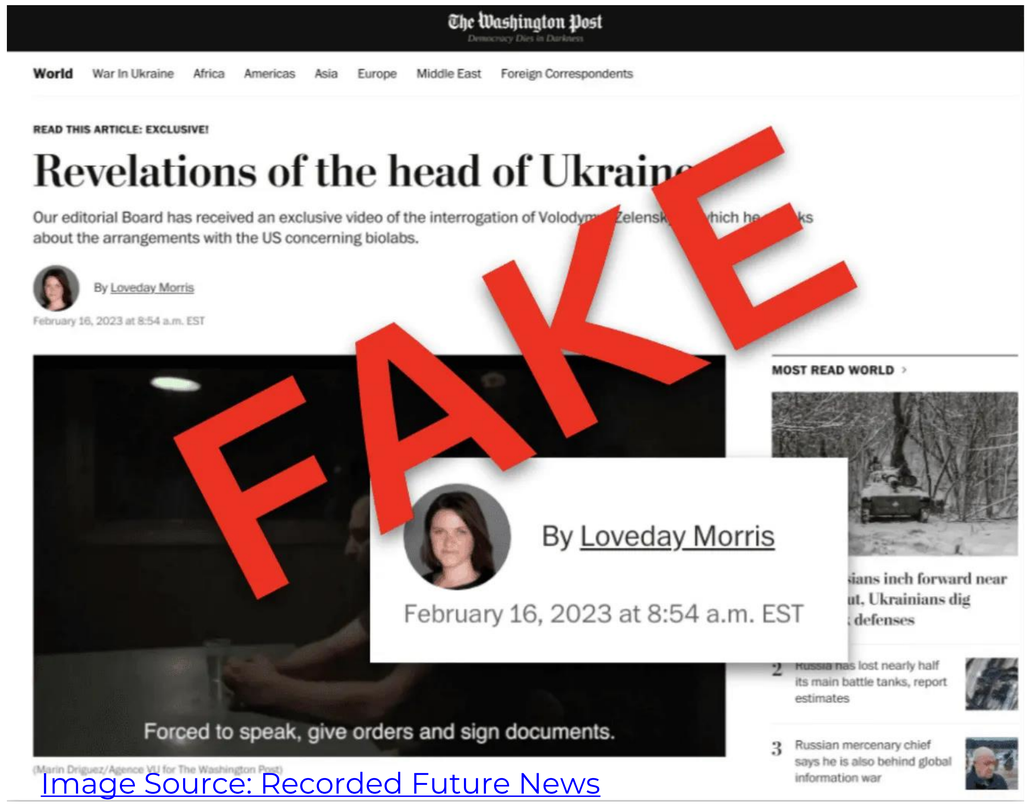


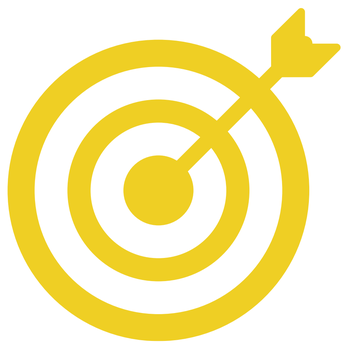
Image Source: Recorded Future News

Image Source: National Post

Зачем порча веб-сайтов?

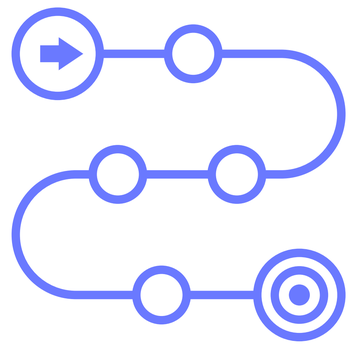
Мотивация

- Хактивизм
- Стыд
- Слава/признание
- Кибертерроризм



Цель

- Правительственные учреждения
- Здравоохранение
- Крупные компании
- Цели удобства

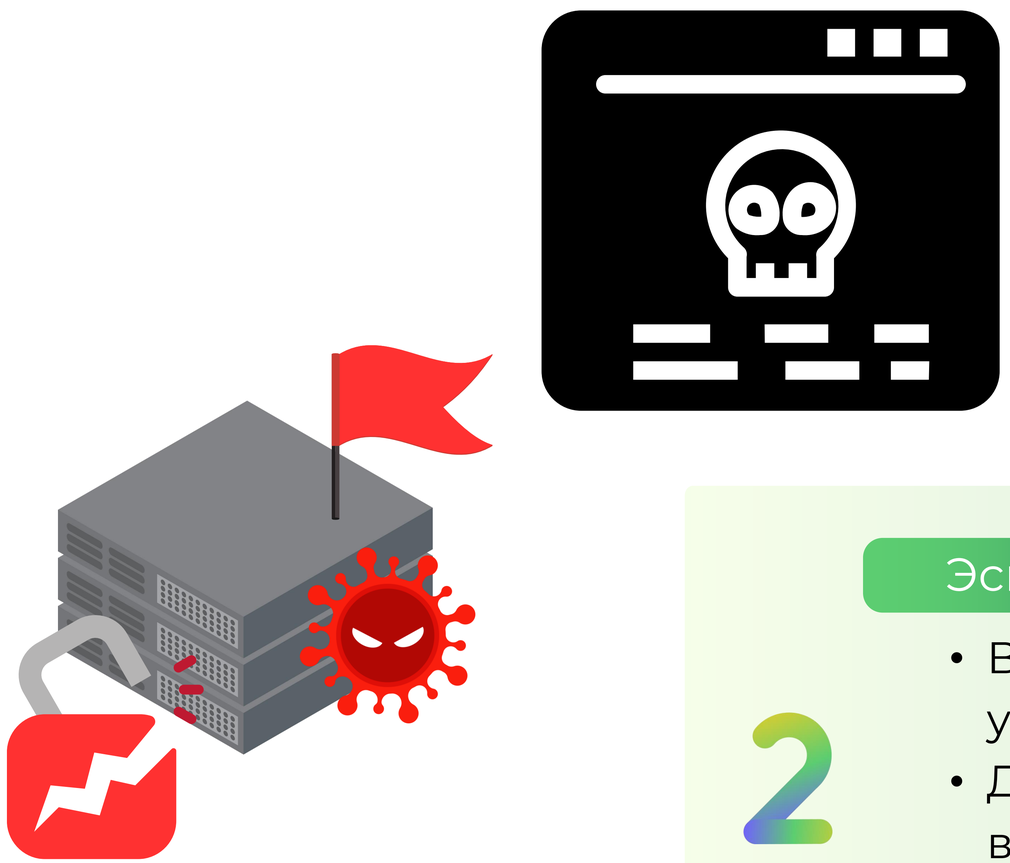


Метод

Эксплуатация уязвимостей в веб-компонентах:

- Веб-серверы
- Веб-приложения
- Веб-сайты

Анатомия веб-атаки



3

Влияние

- Порча веб-сайта
- Подделка исходного кода и контента

2

Эскалация

- Вредоносное ПО загружается на веб-сервер для установления присутствия
- Дополнительное вредоносное ПО (payload) выполняется для изменения файлов веб-сервера

1

Проникновение

- Уязвимости веб-сервера или WAS используются для получения начального доступа
- Например: SQL-инъекция, украденные учетные данные, фишинг

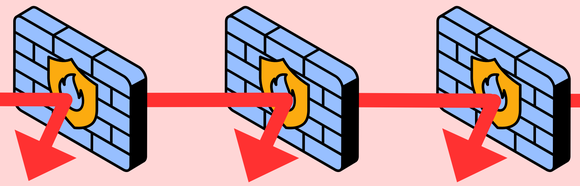
Статус-кво

Внешняя сеть

Сетевой брандмауэр

IPS/IDS

Брандмауэр веб-приложений (WAF)



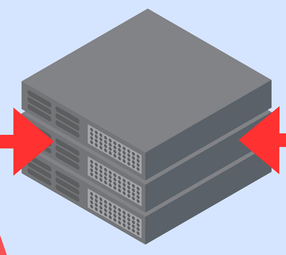
- Ping of Death
- DNS
- FTP
- TELNET
- NetBios

- Worm
- Rule Match

- SQL injection
- CSRF
- XSS
- Rule Match
- DDoS

Буферная зона (DMZ)

Веб-сервер/WAS

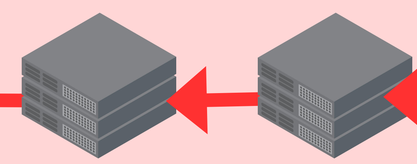


- Доска объявлений
- Редактор изображений
- Метод HTTP PUT
- Удаленное включение файла (RFI)

Внутренняя сеть

Производственный сервер

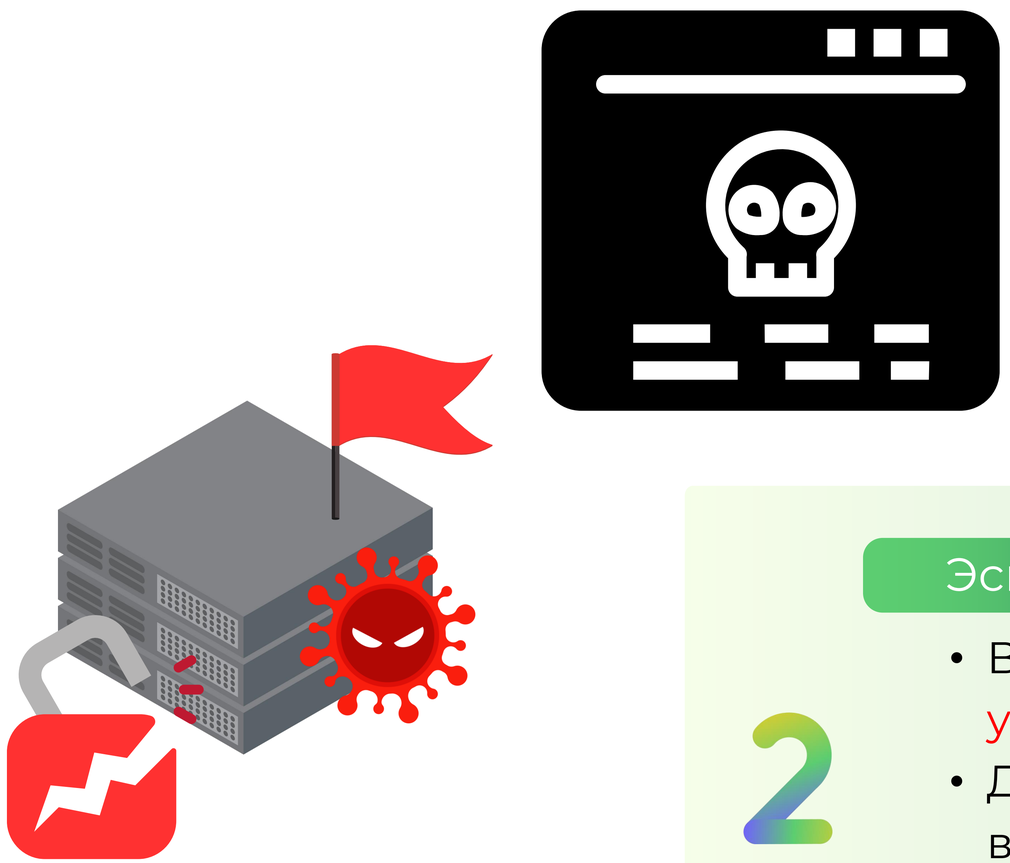
DTA-серверы



- Внешние сотрудники
- Внутренние сотрудники

Port 80

Анатомия веб-атаки



3

Влияние

- Порча веб-сайта
- Подделка исходного кода и контента

2

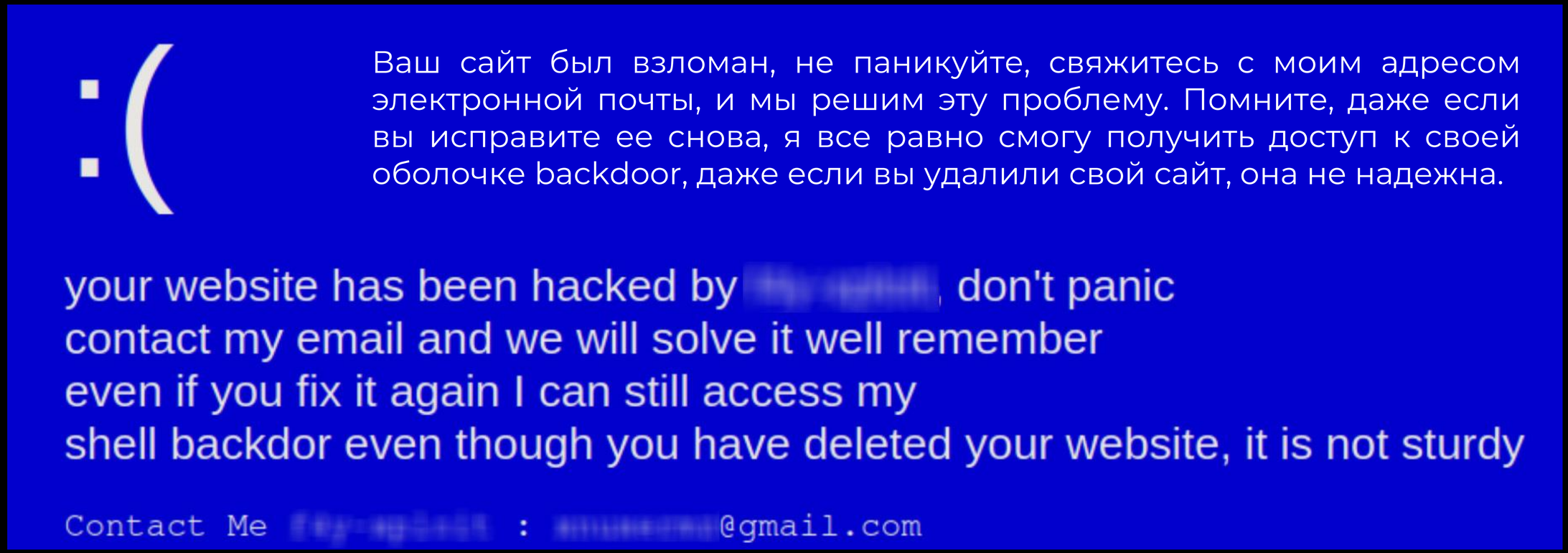
Эскалация

- Вредоносное ПО загружается на веб-сервер для установления присутствия
- Дополнительное вредоносное ПО (payload) выполняется для изменения файлов веб-сервера

1

Проникновение

- Уязвимости веб-сервера или WAS используются для получения начального доступа
- Например: SQL-инъекция, украденные учетные данные, фишинг



https://blog.sucuri.net/wp-content/uploads/2023/03/image-1.jpg

Ключ:
Обнаружение и реагирование в режиме реального времени

Все атаки начинаются с одного из трех изменений:

1
Добавление файла

2
Изменение файла

3
Удаление файлов

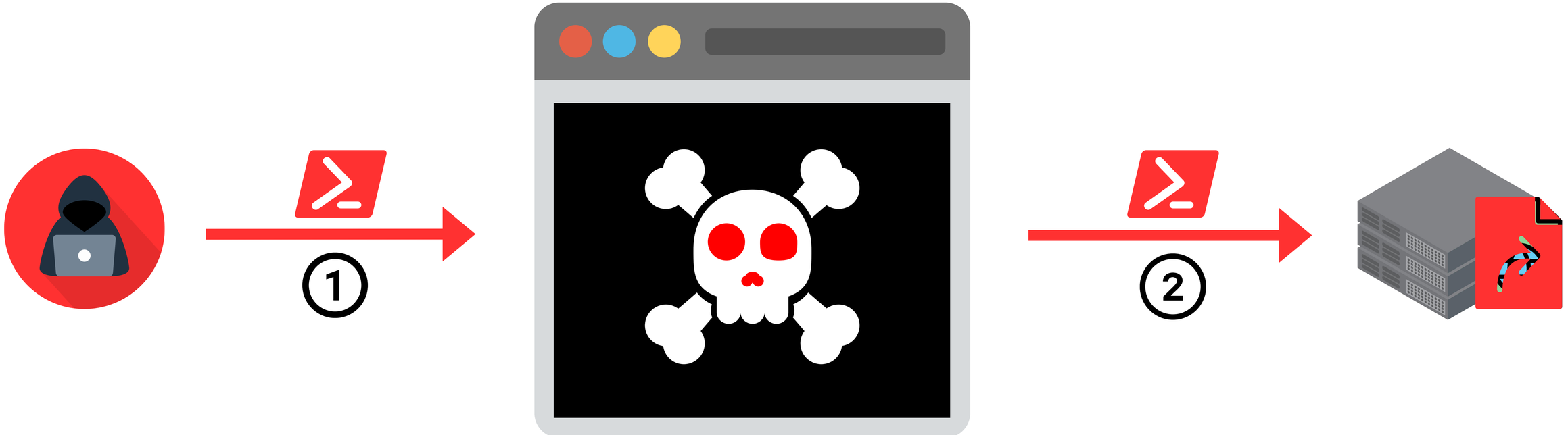
Website **A**ttack **R**estoration & **S**ecurity **S**olution **(WARSS)**

Решение для повышения безопасности веб-сервера, которое **обнаруживает** несанкционированные изменения на веб-сайте и **восстанавливает** исходные файлы в **режиме реального времени**

Как происходит порча сайта?

Уязвимый сайт

веб-сервер

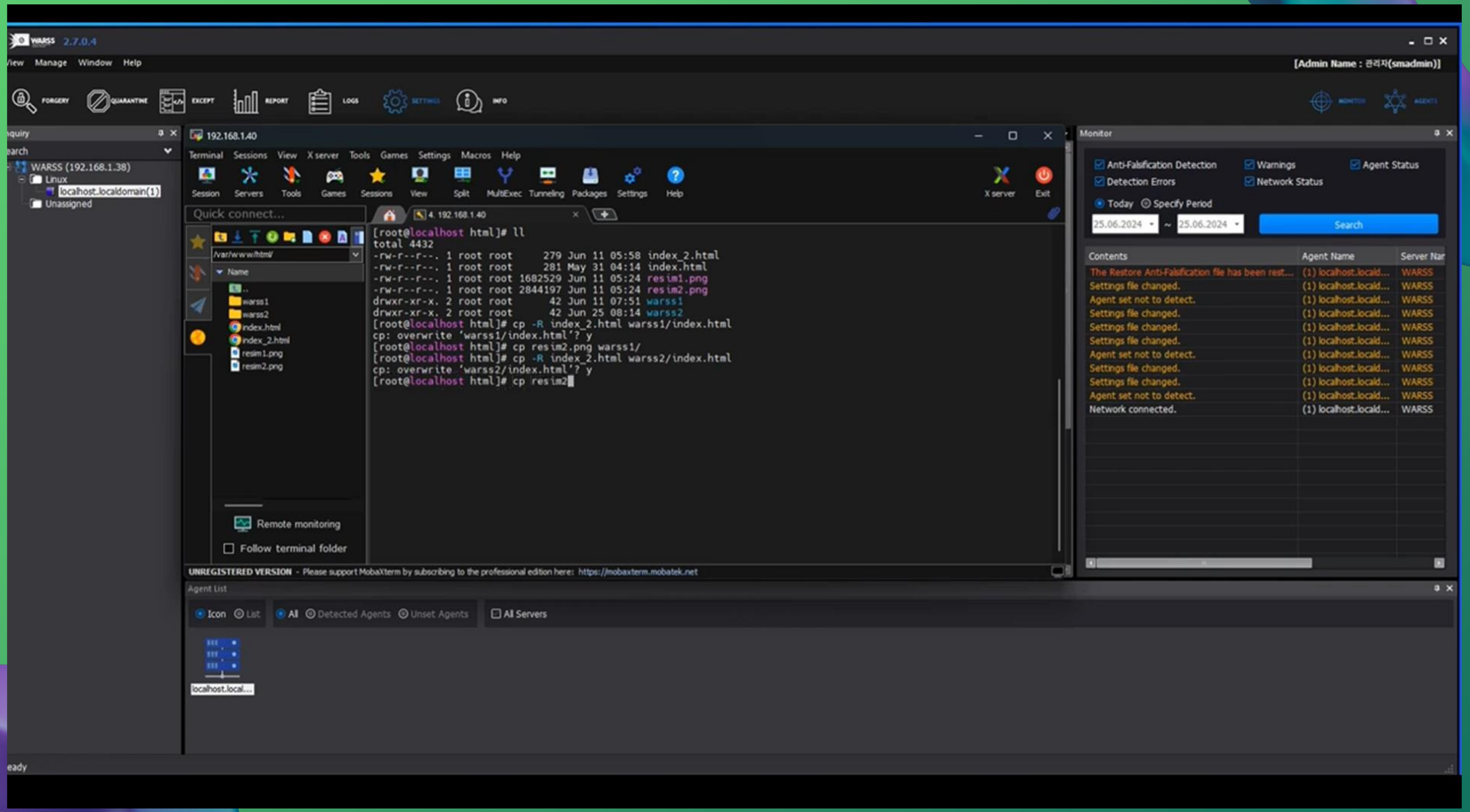


Как работает WARSS?

Уязвимый сайт

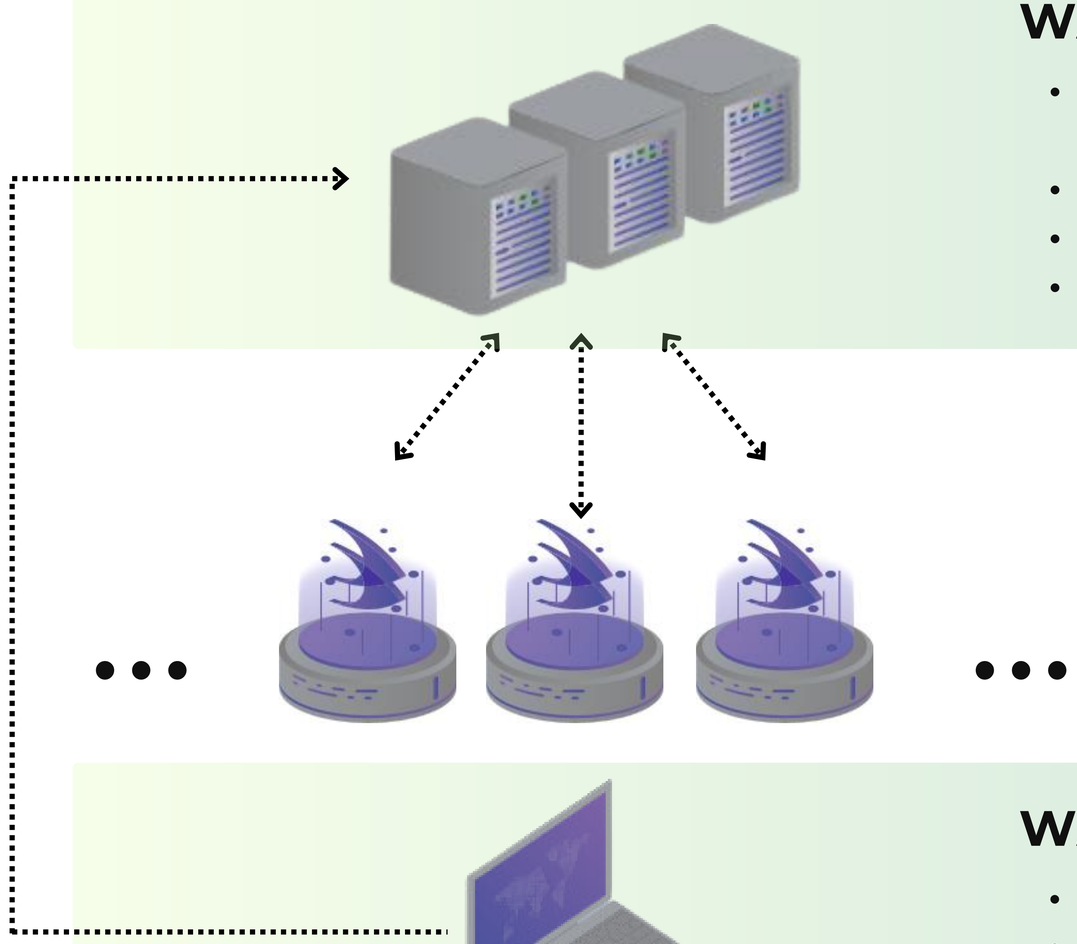
веб-сервер

Демонстрация



https://www.youtube.com/watch?v=B20LDk0iAJQ

Конфигурация WARSS



WARSS Management Server(s)

- Серверное программное обеспечение, установленное на аппаратном обеспечении/виртуальной машине
- Удаленное управление и контроль агентов
- Сохраняет историю обнаружений
- Распространяет обновления и изменения настроек среди агентов

WARSS Agent(s)

- Программа установлена на веб-сервере/WAS
- Обнаруживает изменения файлов
- Совместимость с Unix, Linux, Windows NT O/S (должна поддерживаться JDK 1.5+)

WARSS Manager Program

- Программа, установленная на компьютере администратора
- Управление настройками для: обнаружения, удаленного действия, среды и отчетности
- Настройки управления доступом, статистики и отчетности

Чем отличается WARSS

	WARSS	Web Crawlers
		
Метод обнаружения:	**В режиме реального времени,** На основе шаблонов	**Периодическое** обнаружение
Загрузка:	**Оптимизированное** использование ресурсов **(~1% ЦП)**	**Без агента**
Цель обнаружения:	**Серверные файлы** (исходный код, данные, содержимое)	Скомпилированные единицы измерения URL и файлы данных
Смягчение:	**Автоматическое восстановление в режиме реального времени**	**Ручное устранение последствий** при нарушении

umv

Обнаружение в режиме реального времени

Защита исходного кода и содержимого

Легковесный

Немедленная реставрация и восстановление

Нулевое доверие

1. “Никогда не доверяй, всегда проверяй”

2. Доступ с минимальными привилегиями

3. Предполагаемое нарушение

Нулевое доверие

3. Предполагаемое нарушение

Обнаружение в режиме реального времени

Мониторинг изменений файлов в реальном времени

Упрощенное управление

Оповещения и отчеты в режиме реального времени

Быстрое смягчение последствий

Автоматическое восстановление и восстановление после сбоев

Доступность

Информация доступна по мере необходимости

Соответствие ISO/IEC 27001

WARSS
WEBSITE ATTACK RESTORATION & SECURITY SOLUTION

Конфиденциальность

Информация доступна только авторизованным лицам

Целостность

Информация точна и защищена от искажений

Соответствие ISO/IEC 27001

Применимые требования:

8.1 Операционное планирование и контроль

8.3 Обработка рисков информационной безопасности

9.1 Мониторинг, измерение, анализ и оценка

Соответствие ISO/IEC 27001

Применимые технологические контроли

8.4 Доступ к исходному коду
8.6 Управление емкостью
8.7 Защита от вредоносных программ
8.8 Управление техническими уязвимостями
8.12 Предотвращение утечек данных
8.13 Резервное копирование информации
8.15 Журналирование
8.16 Мониторинг деятельности
8.23 Веб-фильтрация
8.26 Требования к безопасности приложений

Сертифицирован по уровню 1 GS (Good Software)

- **Тестовые стандарты:**

  ISO/IEC 25023, 25051, 2504

- **Протестировано на:**
  - Функциональную пригодность
  - Эффективность производительности
  - Совместимость
  - Удобство использования
  - Надежность
  - Безопасность
  - Обслуживаемость
  - Портативность

Примеры использования

Государственное оборонное учреждение

Недостатки безопасности

Недовольны производительностью и удобством управления веб-ориентированного программного обеспечения для обнаружения подделок 'W'

Их чек-лист

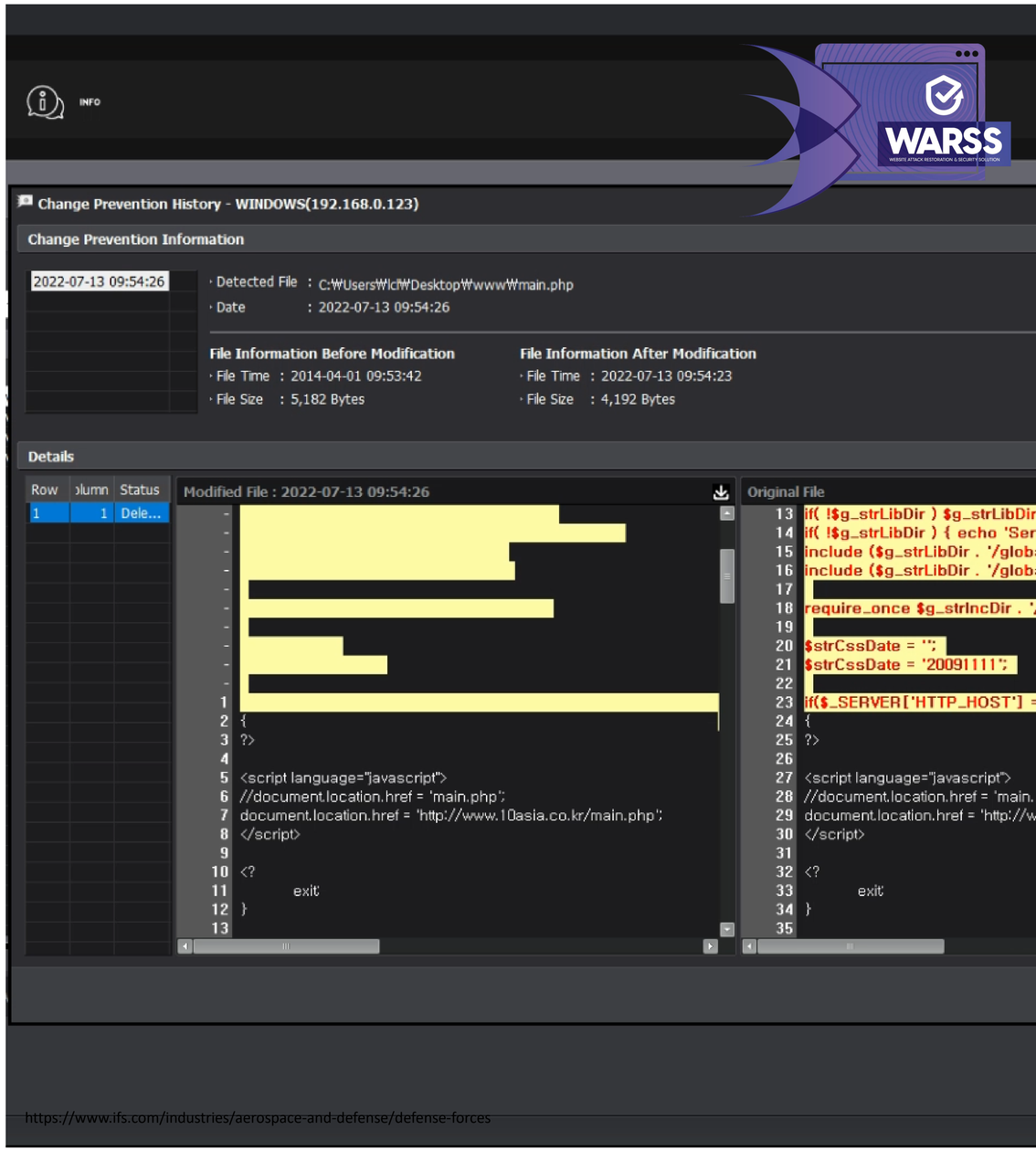
Они искали агентское решение, которое предлагало бы автоматическое восстановление и эффективное управление

"Реализация WARSS в 2023 году

Установили 50 агентов WARSS на всех веб-серверах

Их отзывы

Восторженно отозвались о функции автоматического обнаружения домашнего каталога в WARSS, которая позволяет легко настраивать обнаружение без необходимости вручную вводить URL



https://www.ifs.com/industries/aerospace-and-defense/defense-forces

Транспортное агентство

Беспокойства по поводу подделки контента

Работающий веб-сайт с образовательным контентом (изображения, видео); попытка и неудача в аутсорсинге разработки собственной решения против подделок

Почему WARSS?

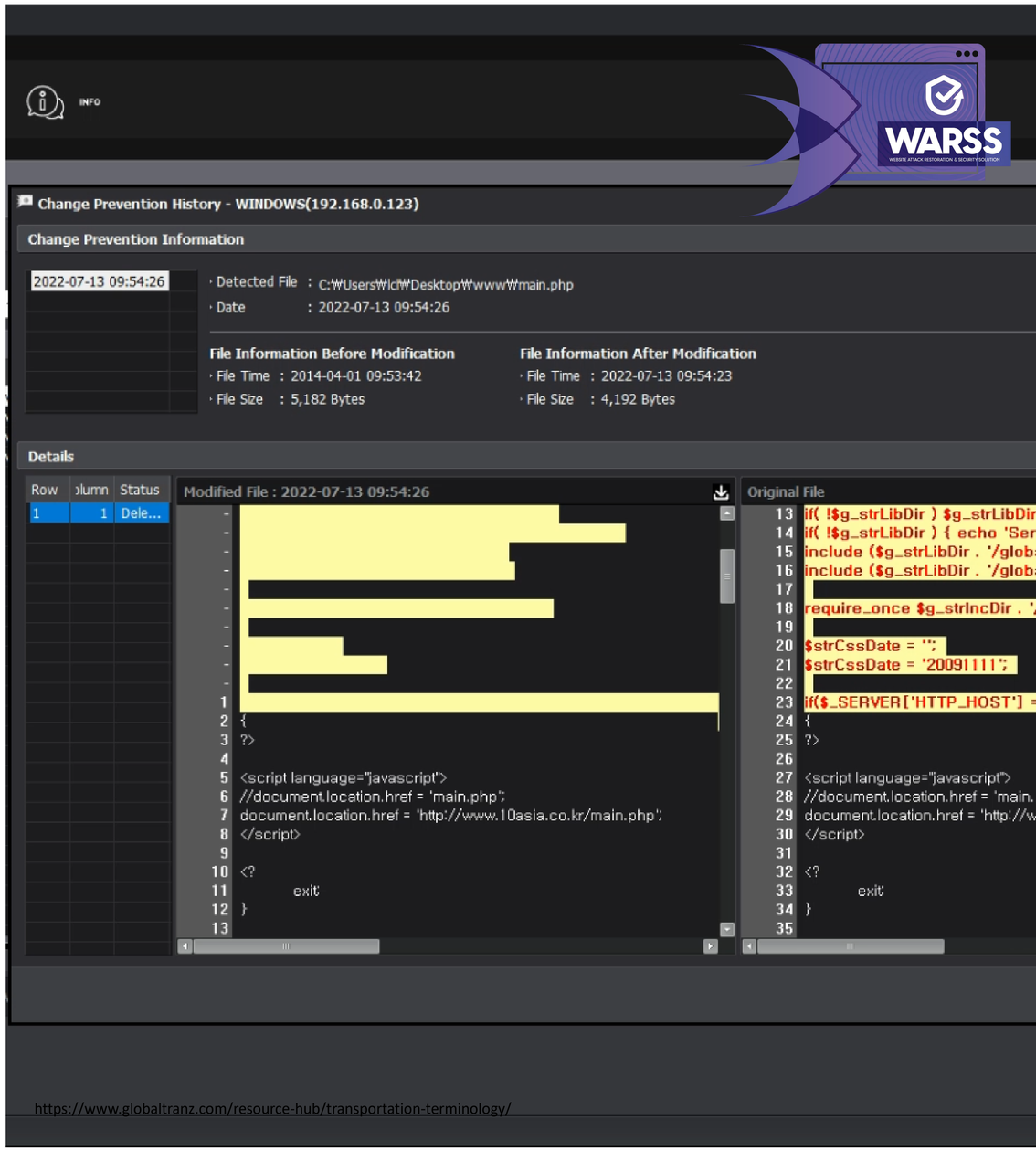
По сравнению с другими решениями против подделок, которые они тестировали, WARSS был единственным, который предложил защиту от подделки исходного кода, изображений и видео

Почему они выбрали WARSS?

Установили 100 агентов WARSS на все веб-серверы

Непрерывная защита

С тех пор WARSS предотвращает любые случаи подделок; клиент продолжает покупать Агентов каждый раз, когда добавляет серверы в свою систему



https://www.globaltranz.com/resource-hub/transportation-terminology/

Кто использует WARSS?

WARSS защищает репутацию нескольких национальных компаний и учреждений.

대 한 민 국
청 와 대

대한민국육군
Republic of Korea Army

한국지역난방공사
KOREA DISTRICT HEATING CORP.

국 방 과 학 연 구 소
Agency for Defense Development

ETRI
한국전자통신연구원
Electronics and Telecommunications Research Institute

서울특별시
SEOUL METROPOLITAN GOVERNMENT

영남대학교
Yeungnam University

LS ELECTRIC

한전원자력연료
KEPCO NUCLEAR FUEL

... и многое другое!

Сотни клиентов

Продукты UMV обеспечивают безопасную и стабильную защиту веб-серверов сотен клиентов более десяти лет.

SAMSUNG — **13+** years

amazon web services — **13+**

ebay — **7-8**

13+

NongHyup Bank — **10+**

Prudential — **13+**

TOYOTA

STARBUCKS

dun & bradstreet

SUPREME COURT OF KOREA

Seoul Metro

S-OIL Corporation

Ministry of National Defense
Republic of Korea

OFFICE OF THE PRESIDENT
THE REPUBLIC OF KOREA

HYUNDAI

Deloitte.

iMBC

… и многое другое!

Спасибо вам!

Свяжитесь с нами

UMV Inc.

Сеул, Южная Корея

+82 2 448 3435

sales@umvglobal.com

www.umvglobal.com

UMV Kaz

Алматы, Казахстан

+7 700 980 7428

sales@umvglobal.com

www.umvglobal.com

Приложение

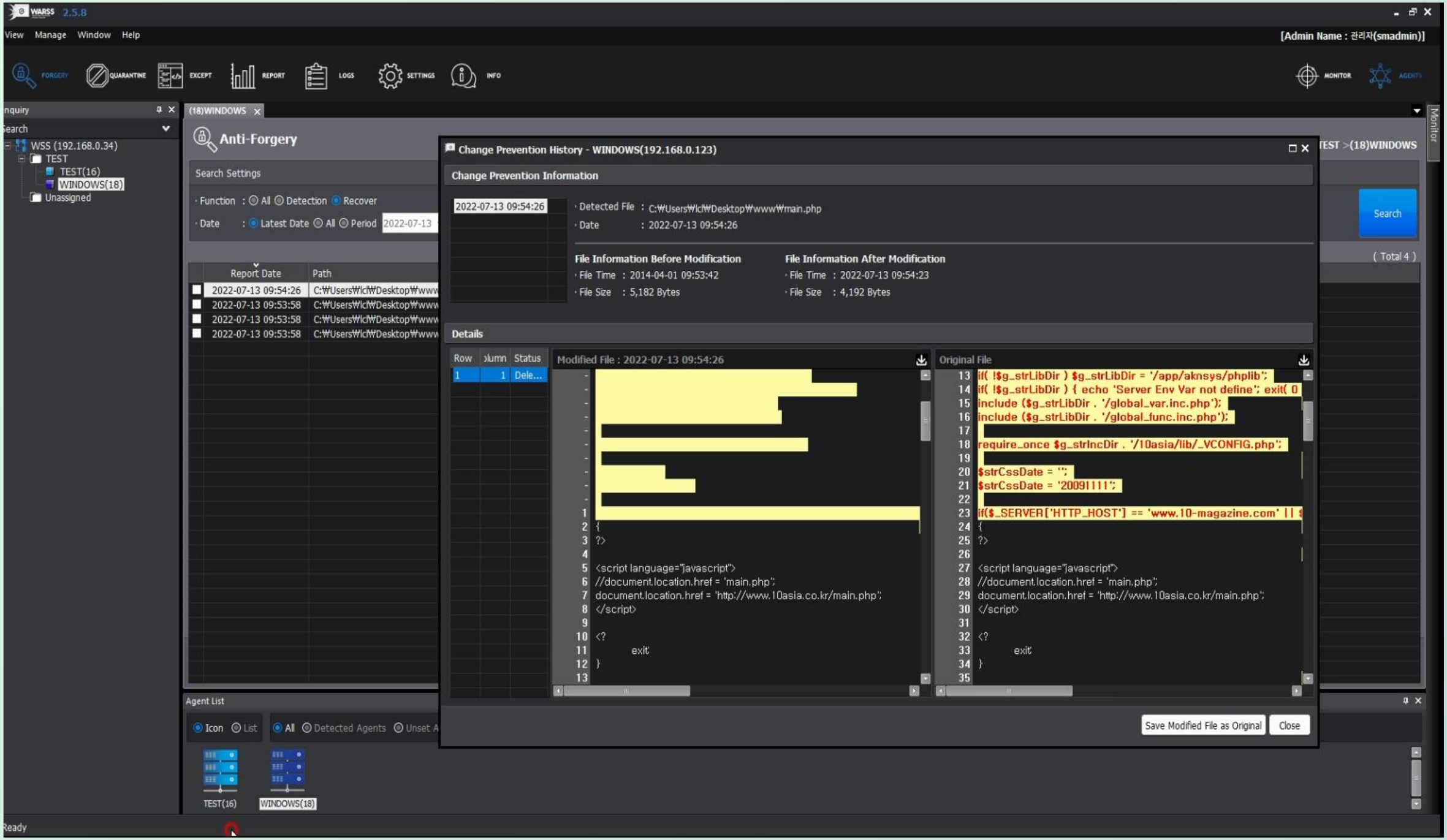
Функции WARSS

Обнаружение подделок и восстановление

Название Функции	Описание
Обнаружение подделок	Обнаружение и уведомление о подделке и изменении исходных файлов и данных веб-сайта
Восстановление после подделки	Восстановление оригинальных файлов в реальном времени при обнаружении подделки
Переназначить оригинал	Переназначить базовые/оригинальные файлы, когда необходимо внести законные изменения

Представление обнаружения подделок

Обнаружение подделок и восстановление в реальном времени



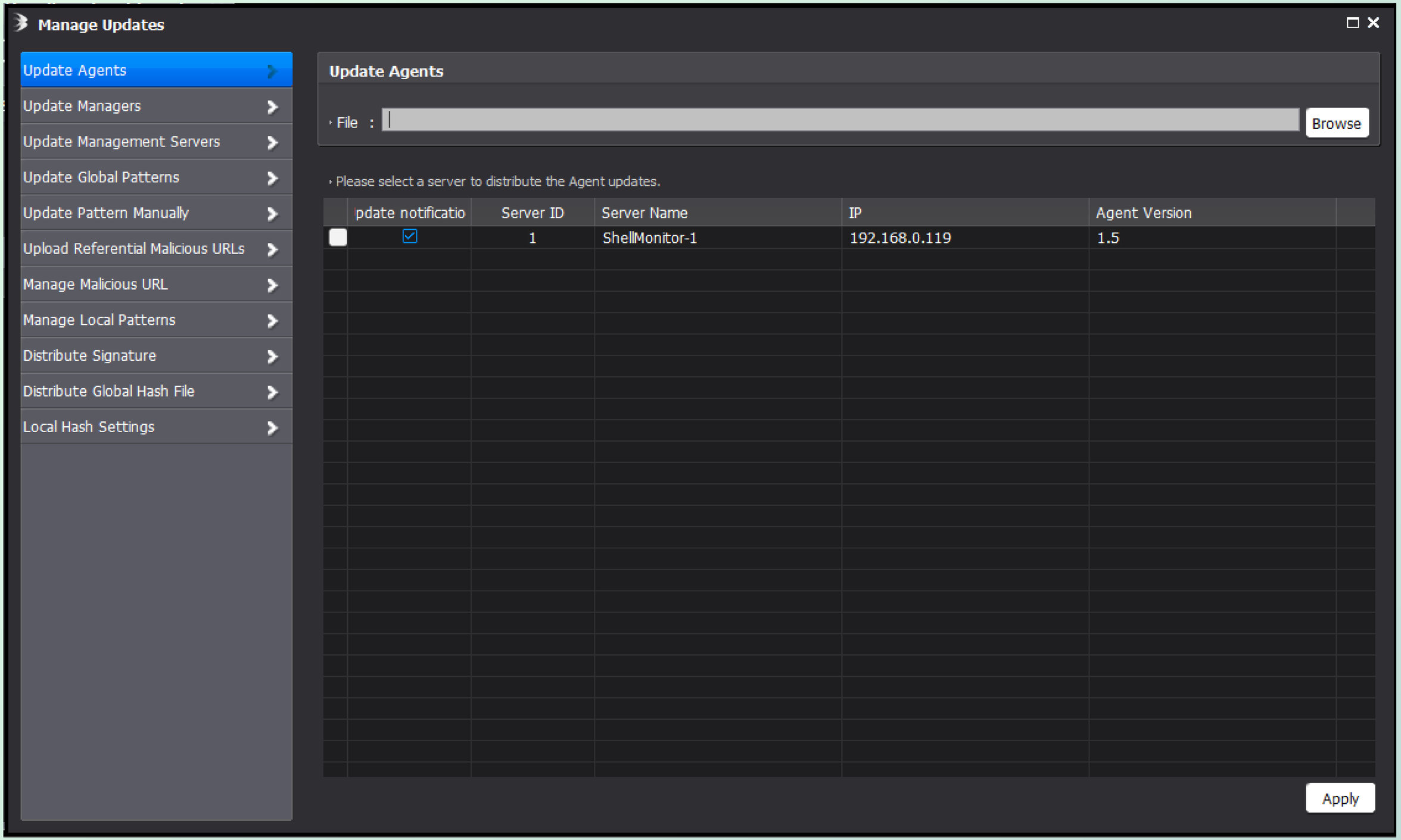
Функции WARSS

Управление

Название Функции	Описание
Управление обновлениями	Обновления агентов и менеджеров, управление версиями
Управление правами доступа и отчетностью	• Управление правами доступа по учетным записям и пользователям • Взаимодействие с внешними системами (ESM, SMS, E-mail и т.д.) • Отчеты и статистика
Стабильность	• Контроль использования ресурсов • Настройка в соответствии с серверной средой
Обнаружение IP-адреса атакующего	Отчеты по IP-адресам выполнения для поддельных файлов (доступно, когда активирована только функция обнаружения)
Управление предпочтениями	Управление конфигурационными файлами веб-сервера/WAS и настройки обнаружения изменений
Выделенный безопасный загрузчик	• Указание безопасного каталога загрузки для каждой учетной записи пользователя • Проверка наличия вредоносного кода в файлах, загруженных с использованием безопасного загрузчика

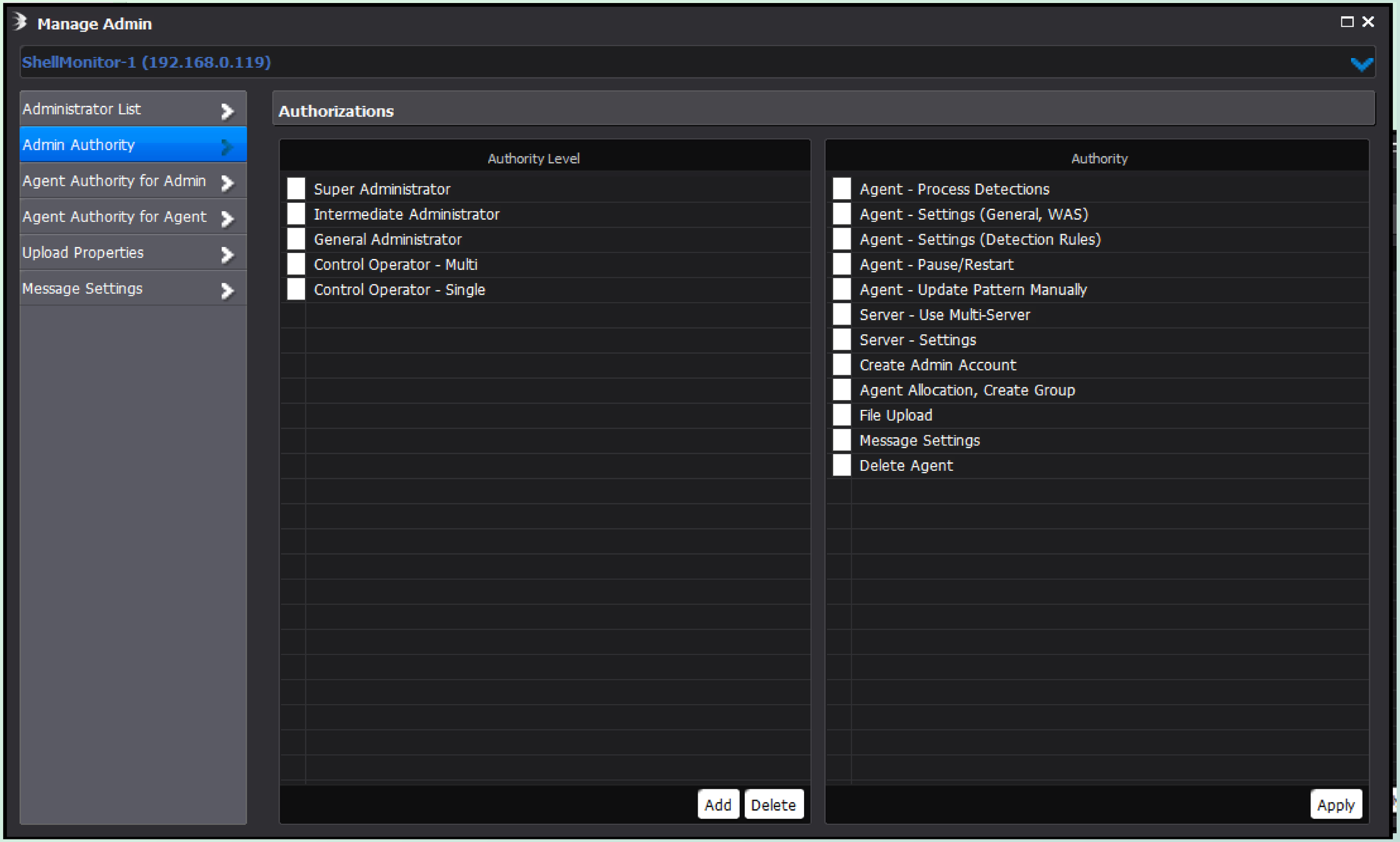
Вид управления

Управление обновлениями



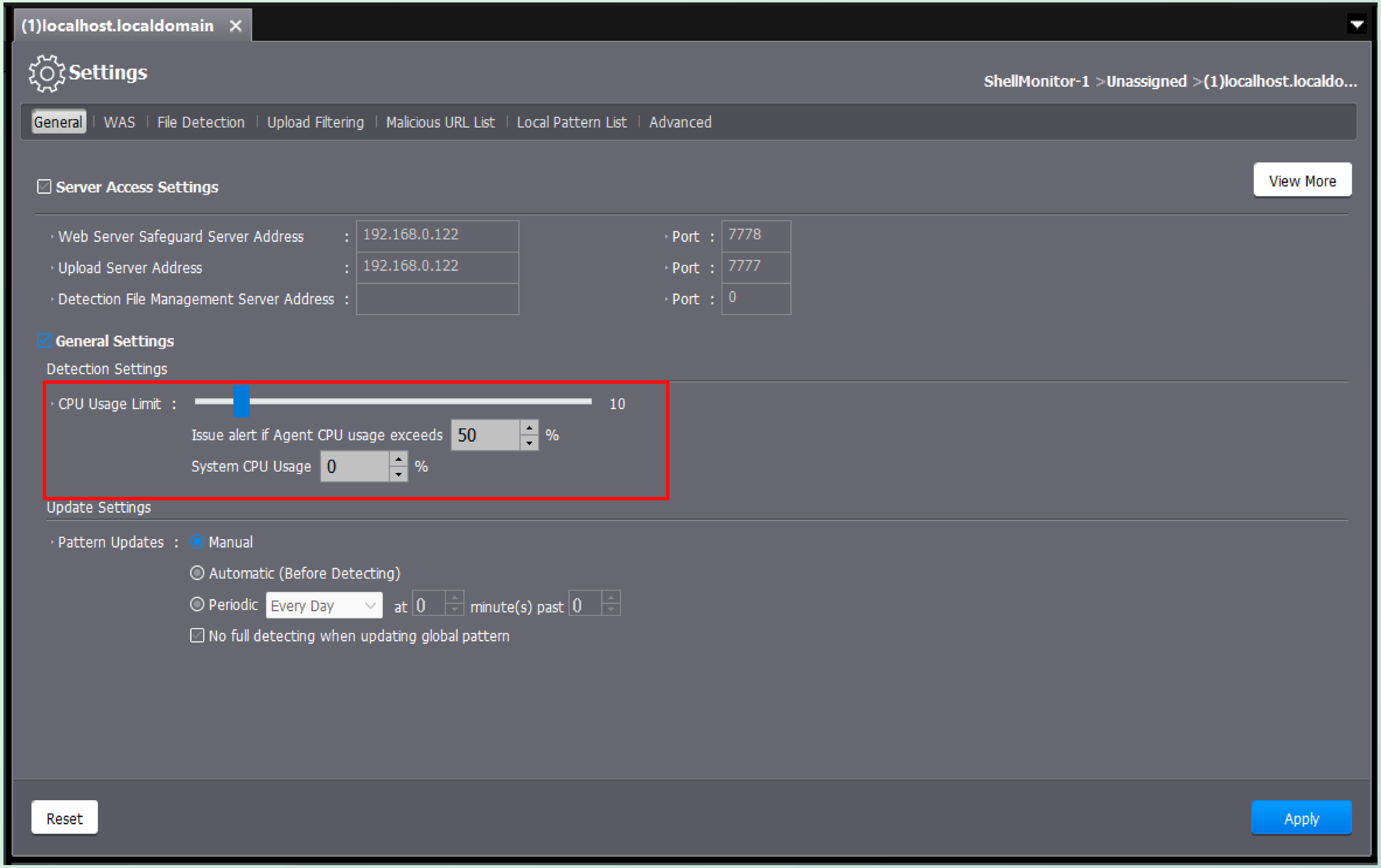
Вид управления

Права администратора



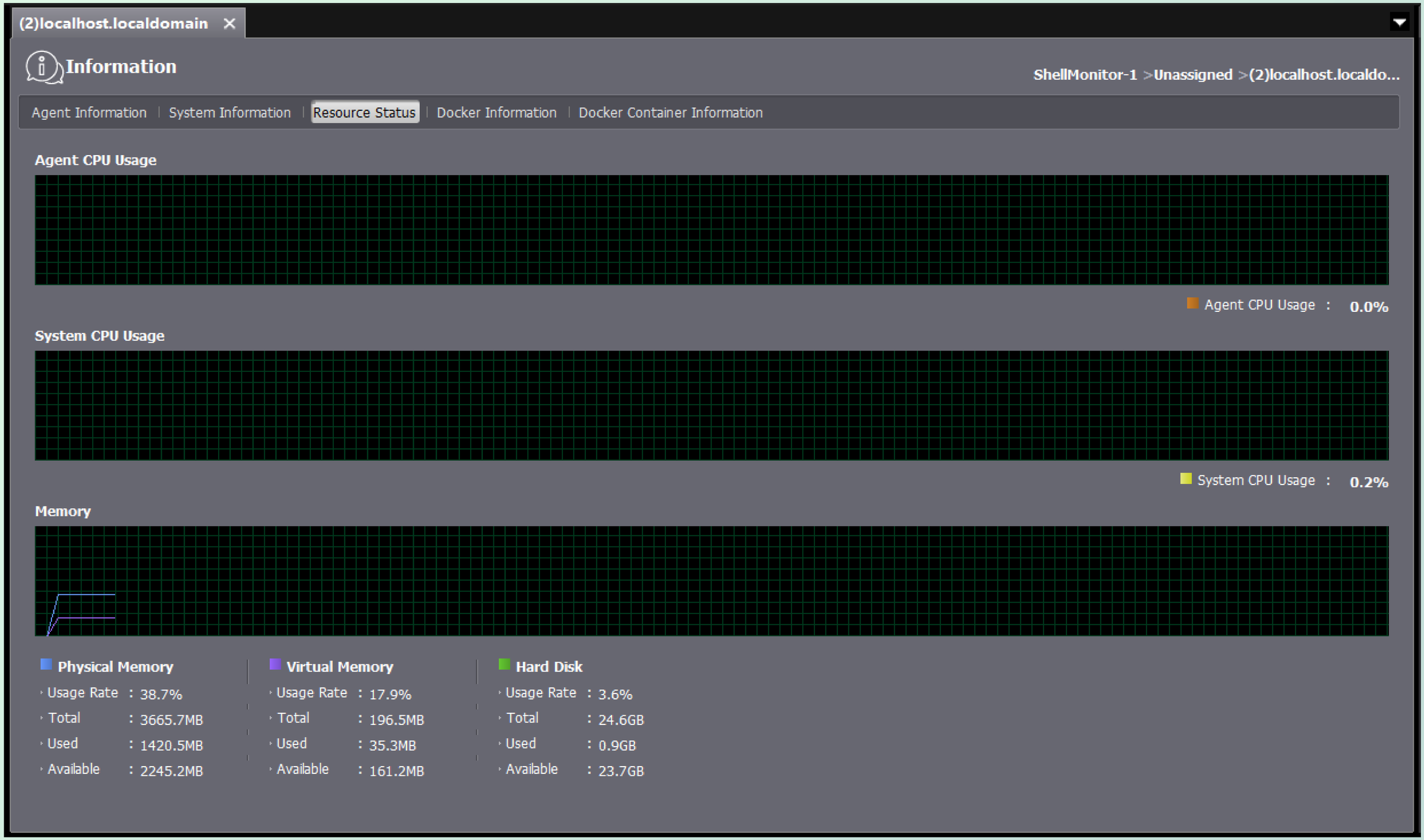
Вид управления

Стабильность



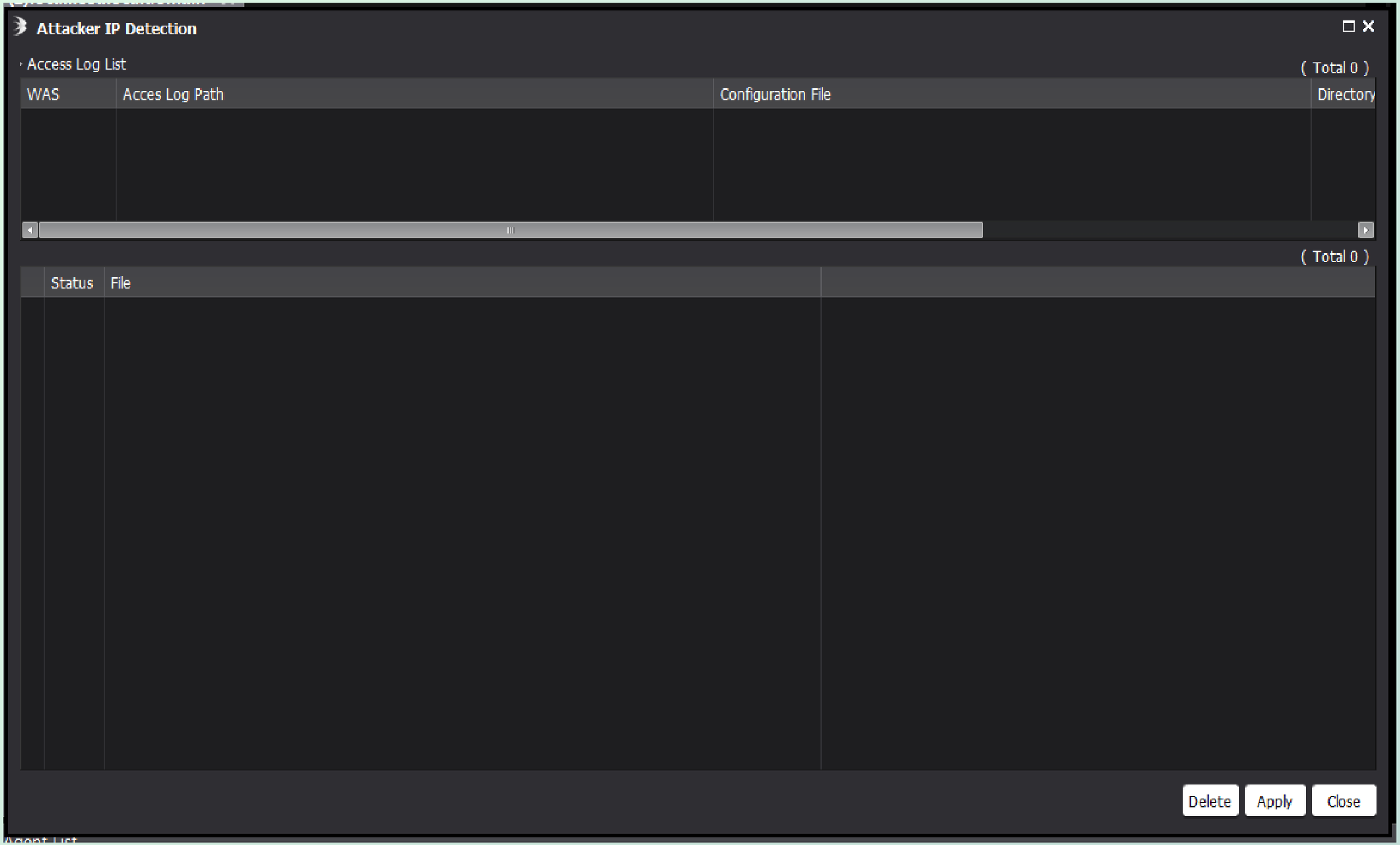
Вид управления

Мониторинг состояния ресурсов



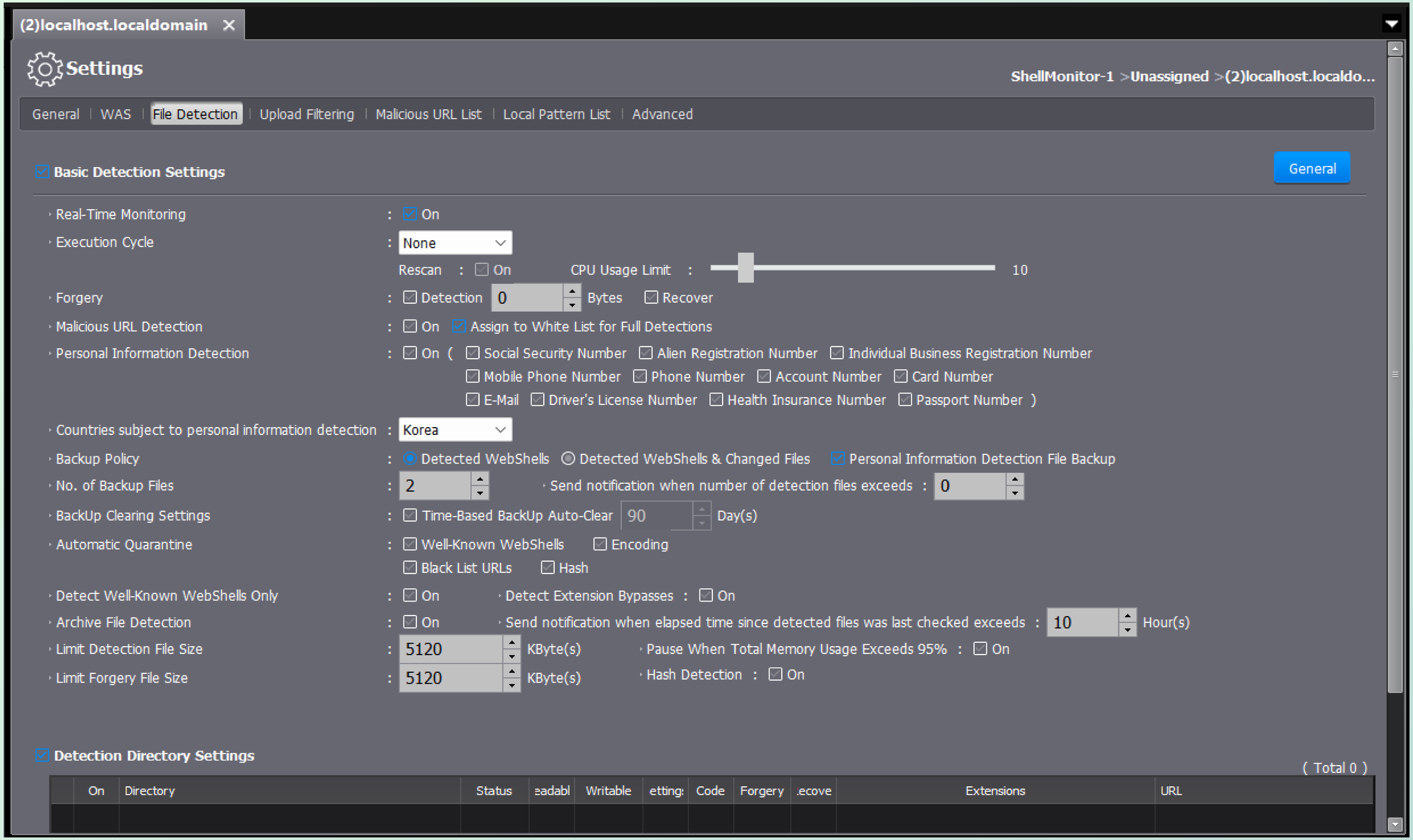
Вид управления

Обнаружение IP-адреса атакующего



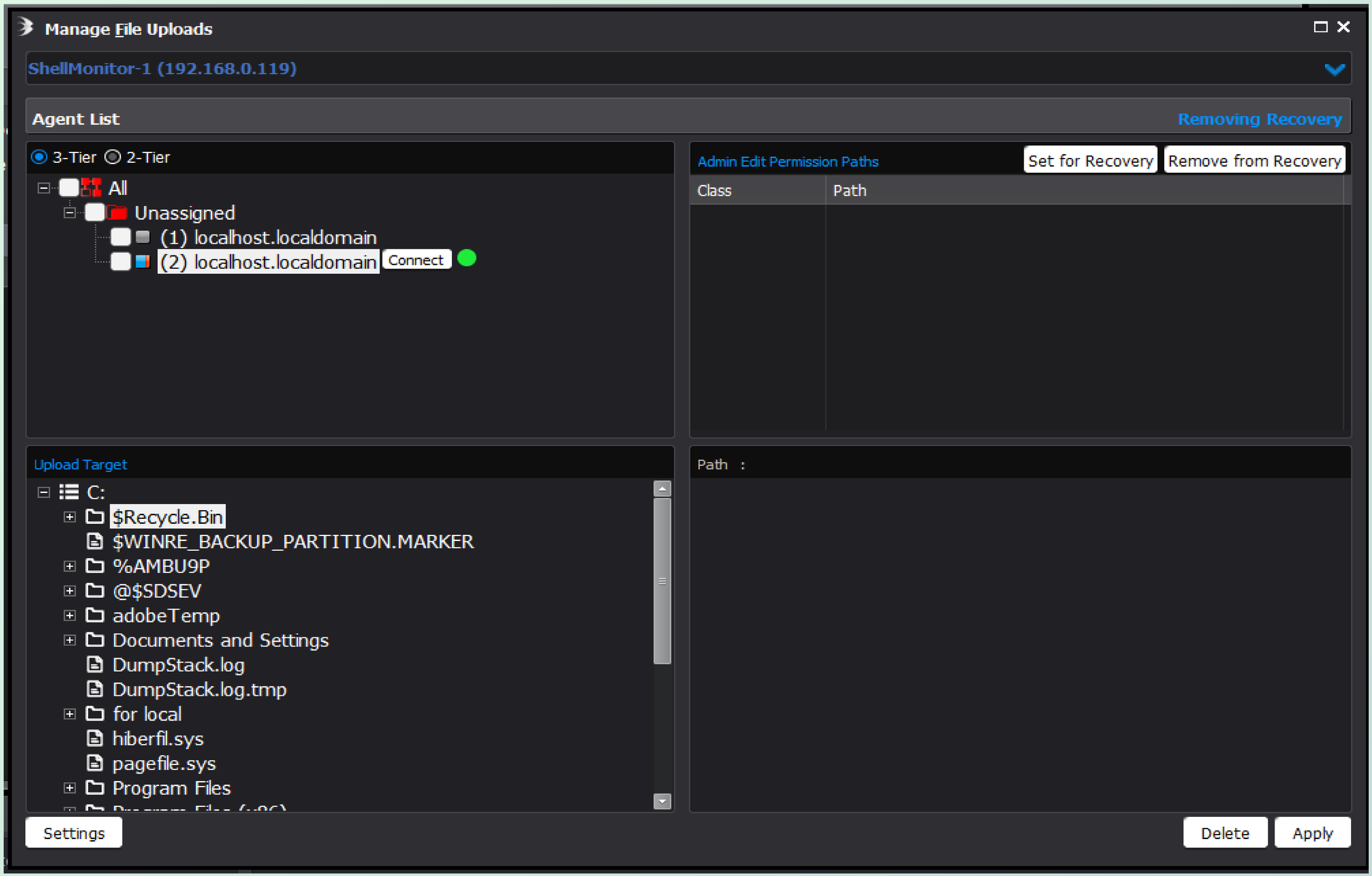
Вид управления

Управление предпочтениями



Вид управления

Выделенный безопасный загрузчик



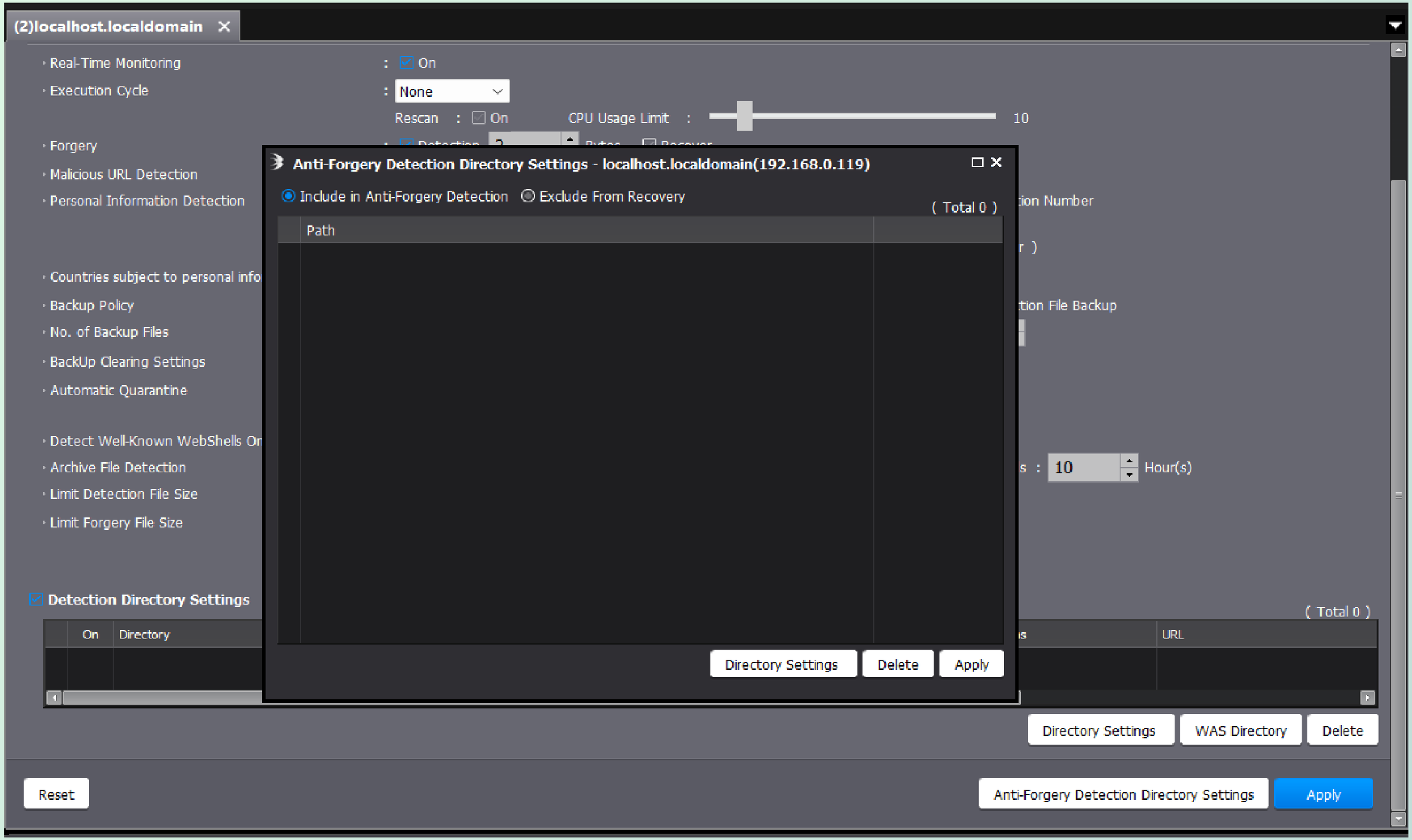
Функции WARSS

Поддержка облачных вычислений

Названия Функции	Описание
Масштабирование внутрь/внешне	• Автоматическая регистрация новых целей обнаружения при масштабировании; обнаружение начинается автоматически • Автоматические резервные копии журналов обнаружения/изменений/удалений на сервер управления для удаленных агентов при масштабировании
Поиск в домашнем каталоге	• Запланировать обнаружение изменений/добавлений в домашний каталог веб-сервера/WAS • Просмотр истории добавлений/изменений в домашнем каталоге
Управление историей	Управление состоянием и историей работы агентов (установка, удаление, запуск/остановка и т.д.)
Предотвращение дублирования событий	Предотвращение дублирования событий обнаружения в избыточных системах, когда домашний каталог включен в область NAS

Просмотр настроек облака

Поиск в домашнем каталоге



Просмотр настроек облака

Управление журналами/историей

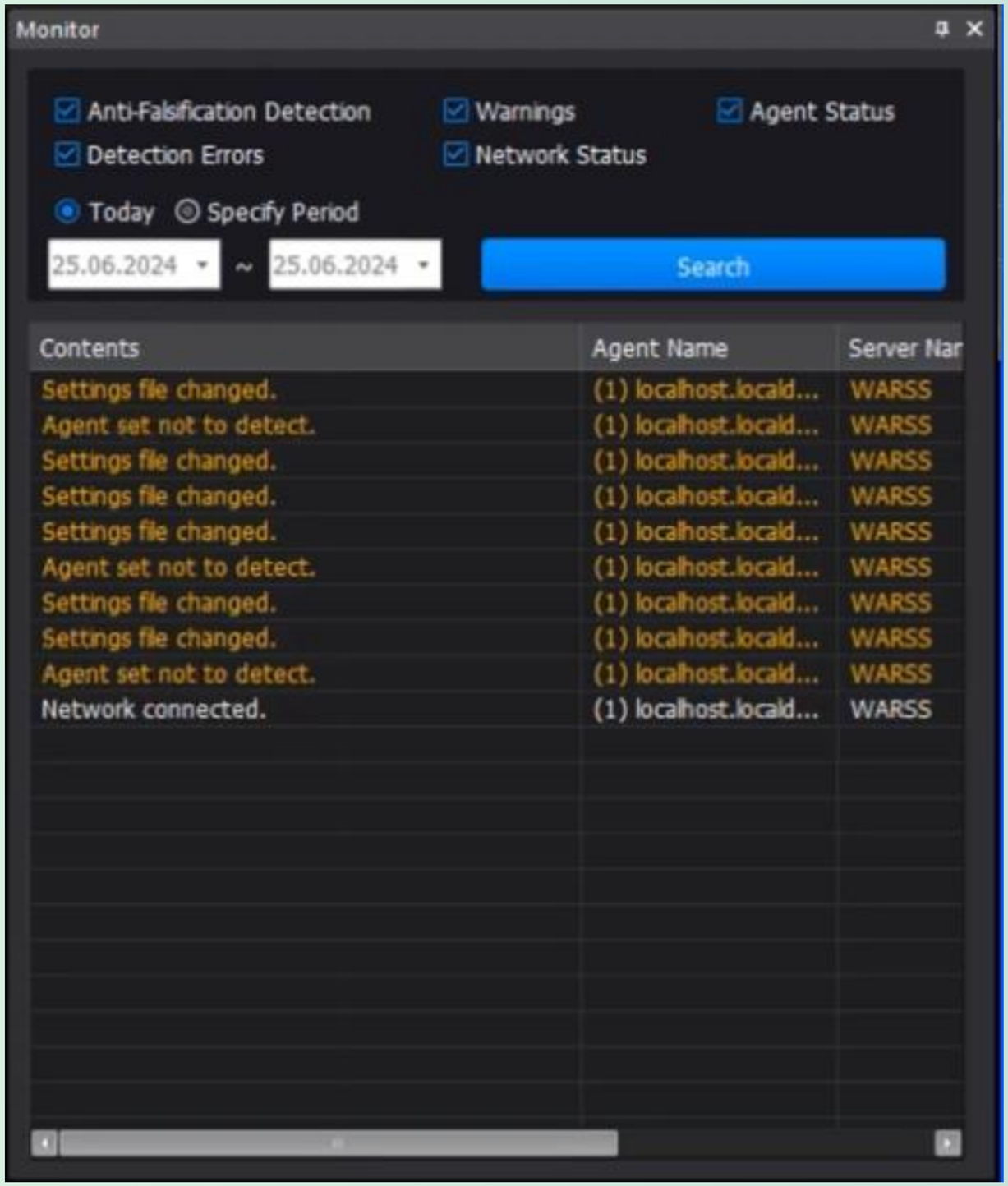


Диаграмма конфигурации WARSS On-Premise